

# Procedure om de AMP-connector te verwijderen als het wachtwoord wordt vergeten

## Inhoud

[Inleiding](#)

[Aansluiting is aangesloten](#)

[Aansluiting is verbroken](#)

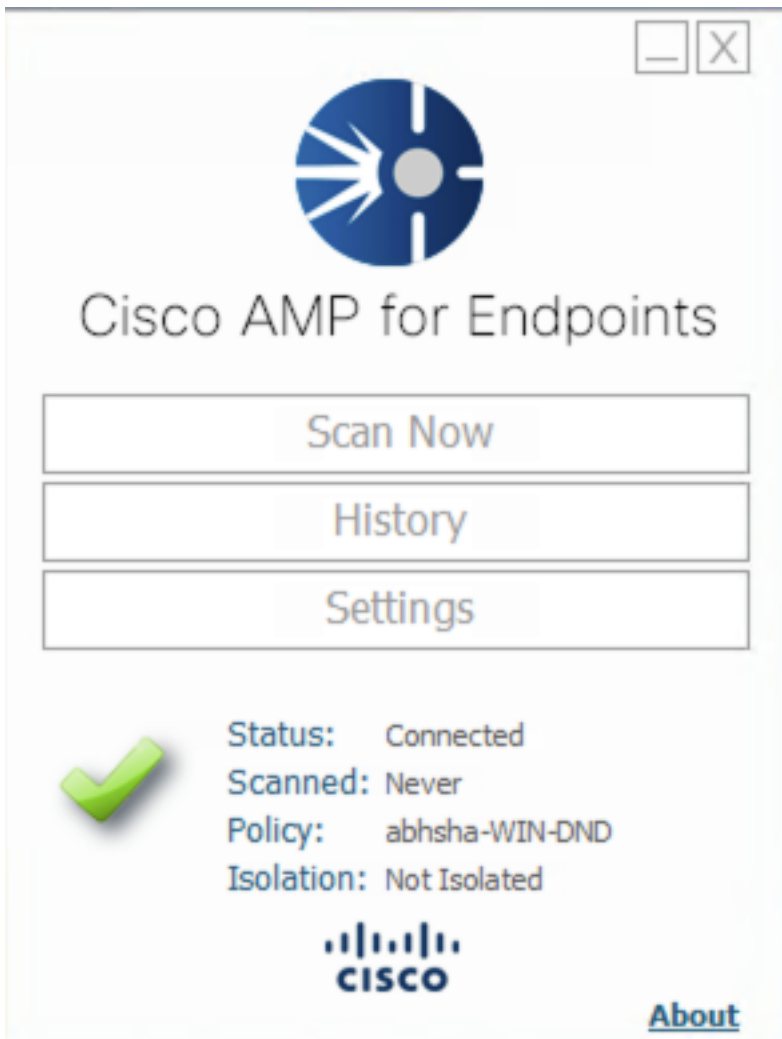
## Inleiding

Dit document beschrijft de procedure om de Cisco Advanced Malware Protection (AMP)-connector te verwijderen als de installatie wordt geblokkeerd door de verbodingsbeveiligingsfunctie waarvoor een wachtwoord moet worden geleverd, en dat wachtwoord wordt vergeten. Er zijn 2 scenario's in dit geval, en dit hangt af van de vraag of de connector "Connected" met de AMP-cloud toont. Het is alleen van toepassing op Windows OS, omdat de connector Protection een functie is die alleen op Windows OS beschikbaar is.

## Aansluiting is aangesloten

Stap 1. Klik op het pictogram en open de Cisco Advanced Malware Protection voor endpoints.

Stap 2. Zorg ervoor dat de connector is zoals aangesloten.



Stap 3. Let op dat het beleid aan die connector is toegewezen.

Stap 4. Navigeer naar uw Advanced Malware Protection voor endpoints en zoek naar het beleid dat eerder is opgemerkt.

Stap 5. Vul het beleid uit en klik op **Duplicaat** zoals in de afbeelding.

Modes and Engines	Exclusions	Proxy	Groups
Files: Quarantine Network: Block Malicious Activity Prot...: Quarantine System Process Protection: Protect	AbhishekSha-TEST Microsoft Windows Default	Not Configured	abhsha-DND
Outbreak Control			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	Not Configured	Not Configured

View Changes Modified 2020-04-23 12:38:35 IST Serial Number 13919

Download XML Duplicate Edit Delete

Stap 6. Een nieuw beleid genaamd "Kopie van.." wordt opgericht. Klik op **Bewerken** om dit beleid te bewerken zoals in de afbeelding.

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	Not Configured
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

[View Changes](#)   Modified 2019-05-21 12:12:01 IST   Serial Number 12267  
 [Download XML](#)   [Duplicate](#)   [Edit](#)   [Delete](#)

Stap 7. Klik op de pagina **Beleid bewerken** op **Geavanceerde instellingen > Administratieve functies**.

Stap 8. In het veld **Wachtwoord voor connectie** vervangt u het wachtwoord door een nieuw wachtwoord dat kan worden opgeroepen zoals in de afbeelding.

**Modes and Engines**

---

**Exclusions**  
2 exclusion sets

---

**Proxy**

---

**Outbreak Control**

---

**Product Updates**

---

**Advanced Settings**

- Administrative Features
- Client User Interface
- File and Process Scan
- Cache
- Endpoint Isolation

- Send User Name in Events i
- Send Filename and Path Info i
- Heartbeat Interval:  i
- Connector Log Level:  i
- Tray Log Level:  i
- Enable Connector Protection i
- Connector Protection Password:  i
- Automated Crash Dump Uploads i
- Command Line Capture i
- Command Line Logging i

Stap 9. Klik op de knop **Opslaan** om dit beleid op te slaan.

Stap 10. Navigeer naar **Management > Groepen** en maak een nieuwe groep aan.

**Groups** [View All Changes](#)

Stap 1. Voer een groepsnaam in en selecteer het **Windows-beleid** als het eerder bewerkte beleid. Klik op de knop **Opslaan** zoals in de afbeelding.

## < New Group

Name	<input type="text" value="TZ-TEST-GROUP"/>
Description	<input type="text"/>
Parent Group	<input type="text"/>
Windows Policy	<input type="text" value="Copy of abhsha-WIN-DND - #1"/>
Android Policy	<input type="text" value="Default Policy (Vanilla Android)"/>
Mac Policy	<input type="text" value="Default Policy (Vanilla OSX)"/>
Linux Policy	<input type="text" value="Default Policy (Vanilla Linux)"/>
Network Policy	<input type="text" value="Default Policy (network_policy)"/>
iOS Policy	<input type="text" value="Default Policy (Audit)"/>

Stap 12. Navigeer naar **Management > Computers** en zoek naar de computer waarop u de AMP-connector wilt verwijderen.

Stap 13. Vul de computer uit en klik op **Verplaatsen naar groep**. Selecteer de laatst gemaakte groep in het dialoogvenster dat nu wordt weergegeven.

DESKTOP-RESMRDG in group abhsha-DND		Definitions Outdated	
Hostname	DESKTOP-RESMRDG	Group	abhsha-DND
Operating System	Windows 10 Pro	Policy	abhsha-WIN-DND
Connector Version	7.2.7.11687	Internal IP	10.197.225.213
Install Date	2020-04-23 12:35:56 IST	External IP	72.163.220.18
Connector GUID	48838c52-f04f-454a-8c3a-5e55f7366775	Last Seen	2020-04-23 12:49:01 IST
Definition Version	TETRA 64 bit (None)	Definitions Last Updated	None
Update Server	tetra-defs.amp.cisco.com		
Processor ID	0fabfbff000006f2		

[Events](#) [Device Trajectory](#) [Diagnostics](#) [View Changes](#)

Stap 14. Wacht tot het beleid op het eindpunt wordt bijgewerkt. Het duurt gewoonlijk ongeveer 30 minuten tot 1 uur en is afhankelijk van het ingestelde interval.

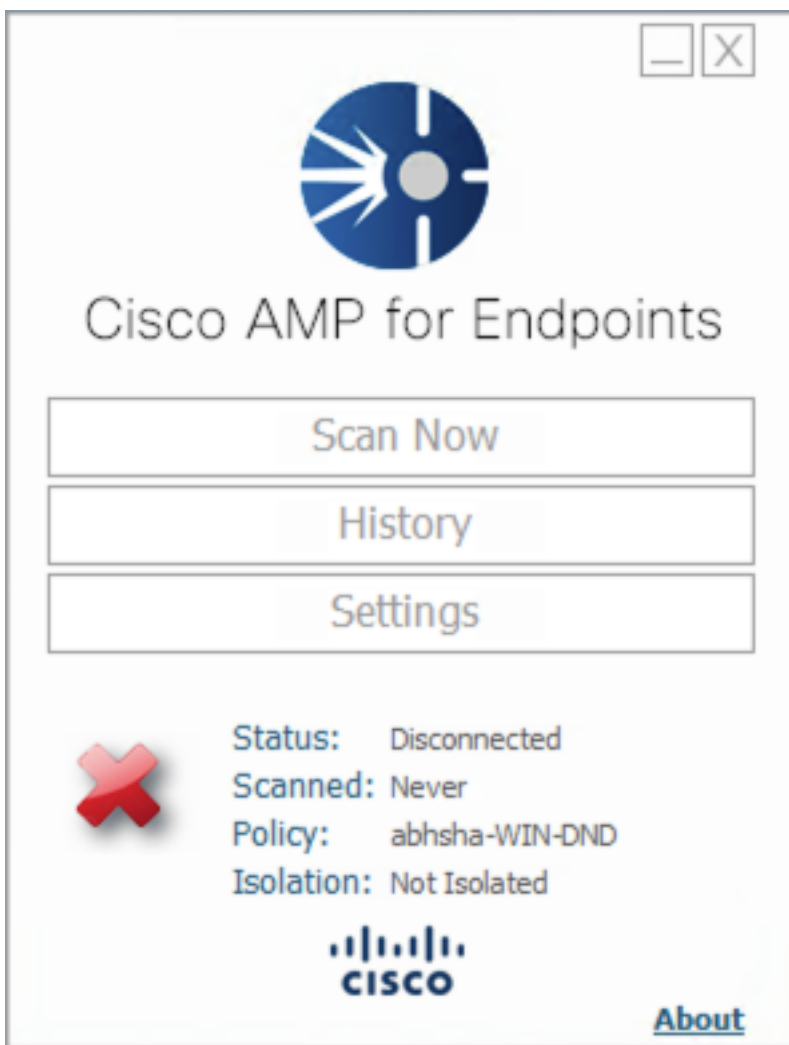
Stap 15. Zodra het beleid op het eindpunt is bijgewerkt, kunt u de connector verwijderen met het wachtwoord dat u onlangs hebt ingesteld.

## Aansluiting is verbroken

Als de connector van de AMP-cloud is losgekoppeld, is het belangrijk om de computer in Safe Mode te kunnen starten.

Stap 1. Klik op het pictogram en open de Cisco Advanced Malware Protection voor endpoints.

Stap 2. Zorg ervoor dat de connector als losgekoppeld is weergegeven.



Stap 3. Let op het beleid dat aan die connector is toegewezen.

Stap 4. Navigeer naar uw Advanced Malware Protection voor endpoints en zoek naar het beleid dat eerder is opgemerkt.

Stap 5. Vul het beleid uit en klik op **Duplicaat** zoals in de afbeelding.

abhsa-WIN-DND 1 2

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	abhsa-DND <span>2</span>
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

[View Changes](#) Modified 2020-04-23 12:38:35 IST Serial Number 13919
 [Download XML](#)

[Duplicate](#)
[Edit](#)
[Delete](#)

Stap 6. Een nieuw beleid genaamd "Kopie van.." wordt opgericht. Klik op **Bewerken** om dit beleid te bewerken.

Copy of abhsa-WIN-DND 0 0

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	Not Configured
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

[View Changes](#) Modified 2019-05-21 12:12:01 IST Serial Number 12267
 [Download XML](#)
[Duplicate](#)
[Edit](#)
[Delete](#)

Stap 7. Klik op de pagina Beleid bewerken op **Geavanceerde instellingen > Administratieve functies**.

Stap 8. In het veld **Wachtwoord voor connectie** vervangt u het wachtwoord door een nieuw wachtwoord dat kan worden opgeroepen.

<b>Modes and Engines</b>	<input checked="" type="checkbox"/> Send User Name in Events <span>i</span>
<b>Exclusions</b> 2 exclusion sets	<input checked="" type="checkbox"/> Send Filename and Path Info <span>i</span>
<b>Proxy</b>	Heartbeat Interval: 15 minutes <span>i</span>
<b>Outbreak Control</b>	Connector Log Level: Debug <span>i</span>
<b>Product Updates</b>	Tray Log Level: Default <span>i</span>
<b>Advanced Settings</b>	<input checked="" type="checkbox"/> Enable Connector Protection <span>i</span>
<b>Administrative Features</b>	Connector Protection Password: .....
Client User Interface	<input checked="" type="checkbox"/> Automated Crash Dump Uploads <span>i</span>
File and Process Scan	<input checked="" type="checkbox"/> Command Line Capture <span>i</span>
Cache	<input type="checkbox"/> Command Line Logging <span>i</span>
Endpoint Isolation	

Stap 9. Klik op de knop **Opslaan** om dit beleid op te slaan.

Stap 10. Navigeer naar **Beheer > Beleid** en zoek naar het nieuwe beleid.

Stap 1. Vul het beleid uit en klik op **Download XML**. Een bestand met de naam **policy.xml** wordt op uw machine opgeslagen.

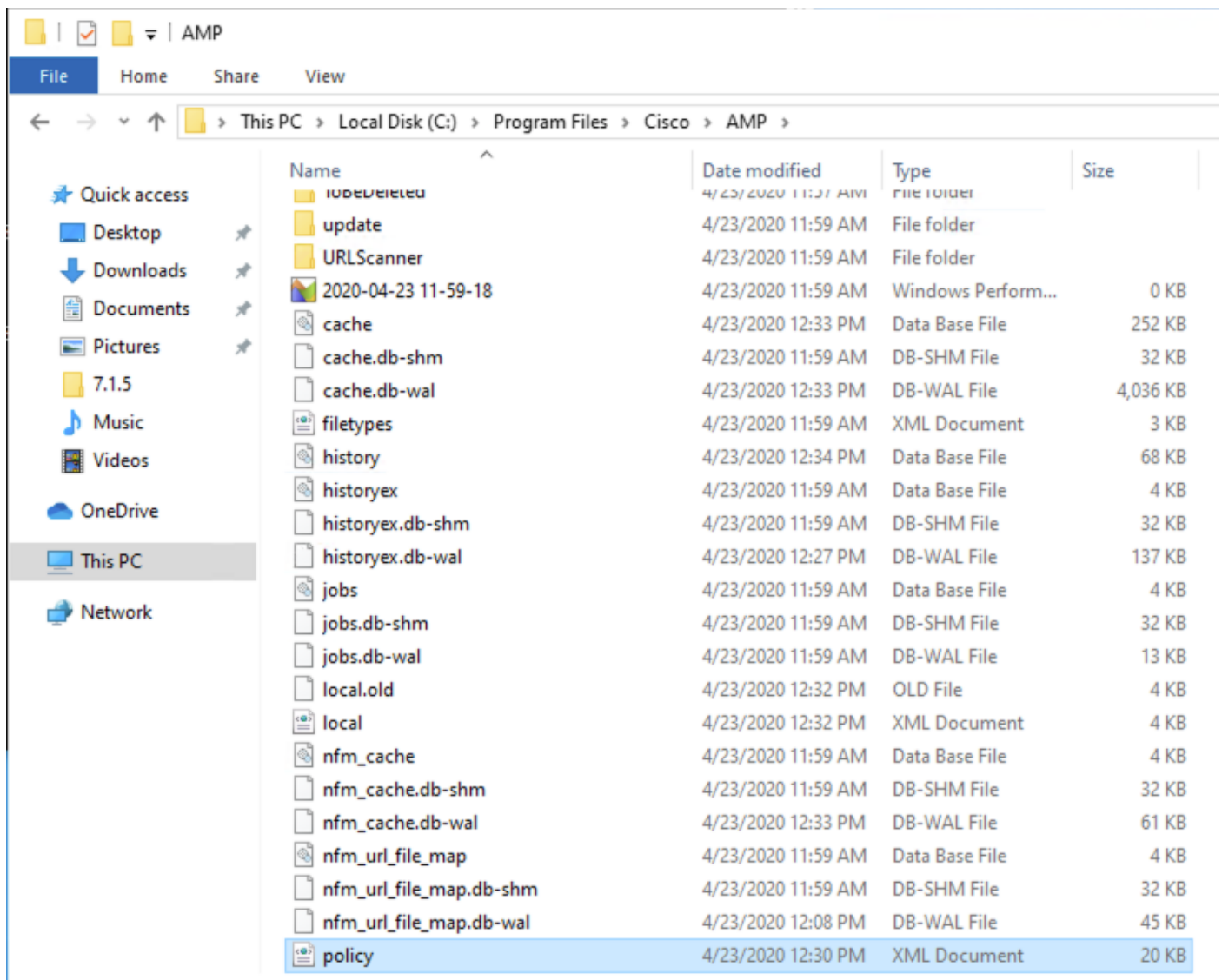
abhsa-WIN-DND <span>1</span> <span>2</span>			
<b>Modes and Engines</b>	<b>Exclusions</b>	<b>Proxy</b>	<b>Groups</b>
Files Network Malicious Activity Prot... System Process Protection	Quarantine Block Quarantine Protect	Not Configured	abhsa-DND <span>2</span>
<b>Outbreak Control</b>			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	Not Configured	Not Configured
View Changes Modified 2020-04-23 12:38:35 IST Serial Number 13919		Download XML	Duplicate Edit Delete

Stap 12. Kopieer dit **beleid.xml** naar het getroffen eindpunt.

Stap 13. Herstart het getroffen eindpunt in **Safe Mode**.

Stap 14. Nadat het getroffen eindpunt in **Safe Mode** is, navigeer dan naar **C:\Program Files\Cisco\AMP**.

Stap 15. In deze map selecteert u een bestand met de naam **policy.xml** en geeft u deze naam aan **policy\_old.xml**.



Stap 16. Plaats nu het eerder gekopieerde **beleid.xml** in deze map.

Stap 17. Nadat het bestand is gekopieerd, kan de installatie normaal gesproken worden uitgevoerd en moet het wachtwoord worden ingevoerd.

Stap 18. Dit is een optionele stap. Aangezien de connector niet is geïnstalleerd toen de machine werd losgekoppeld, blijft de computeringang op de console. Daarom kunt u navigeren naar **Beheer > Computers** en het getroffen eindpunt uitbreiden. Klik op **Verwijderen** om het eindpunt te verwijderen.